CLAIMS

1. Method of inserting a supplementary information item (S), such as a secret watermark, in digital data (I), characterized in that it includes the following steps:

- multi-resolution spectral breakdown (E1) of the digital data;
- extraction (E2) of the components of lowest frequency;
- choice (E3) of a subset of the components of lowest frequency;
- modulation (E4) of the components of said subset in order to insert the supplementary information (S); and
- reverse multi-resolution spectral recomposition (E5) of the watermarked digital data (I').

2. Insertion method according to Claim 1, characterized in that the multi-level spectral breakdown level (d) is predetermined so that the number (n) of components with the lowest frequency is between 8 x 8 and 32 x 32.

3. Insertion method according to one of Claims 1 or 2, characterized in that, at the spectral breakdown step (E1), the spectral breakdown is performed by a discrete wavelet transformation and, at the extraction step (E2), the components of the approximation sub-band (LL) are chosen.

4. Insertion method according to one of Claims 1 or 2, characterized in that, at the spectral breakdown step (E1), the digital data (I) are broken down iteratively into an approximation version corresponding to a low-pass filtering and a sub-sampling of the digital data or of a previous approximation version, and into a detail version corresponding to the subtraction of the approximation version from the digital data or from said previous approximation version, and, at the extraction step (E2), the components of the approximation version are chosen.

5. Insertion method according to one of Claims 1 to 4, characterized in that, at the modulation step (E4), the components of said subset are modulated by adding a modulation value (w_k) generated by a pseudo-random function initialized by a digital signal (S) representing the

supplementary information to be inserted.

6. Insertion method according to one of Claims ~~1 to 5~~, characterized in that, at the choosing step (E3), the subset of components is chosen according to a pseudo-random function initialized by a digital signal (K) representing a confidential key associated with the supplementary information (S) to be inserted.

7. Device for inserting a supplementary information item (S), such as a secret watermark, in digital data (I), characterized in that it has:

- means (11) for the multi-resolution spectral breakdown of the digital data (I);

- extraction means (12) adapted to extract components of lowest frequency;

- choosing means (13) for choosing a subset of the components of lowest frequency;

- means (14) of modulating the components of said subset in order to insert the supplementary information (S); and

- means (15) for the reverse multi-resolution spectral recomposition of the watermarked digital data (I').

8. Insertion device according to Claim 7, characterized in that the multi-resolution spectral breakdown level (d) is predetermined so that the number (n) of components with the lowest frequency is between 8 x 8 and 32 x 32.

9. Insertion device according to one of Claims 7 or 8, characterized in that the multi-resolution spectral breakdown means (11) are adapted to perform a discrete wavelet transformation, the extraction means (12) being adapted to choose the components of the approximation sub-band (LL).

10. Insertion device according to one of Claims 7 or 8, characterized in that the multi-resolution spectral breakdown means (11) are adapted to break down the digital data (I) iteratively into an approximation version corresponding to a low-pass filtering and a sub-sampling of the digital data or of a previous approximation version, and into a detail version corresponding to the subtraction of the approximation version from the digital

data or from said previous approximation version, the extraction means (12) being adapted to choose the components of the approximation version.

11. Insertion device according to one of Claims 7 to 10, characterized in that the modulation means (14) cooperate with a generator (16) of modulation values (w_k) generated by a pseudo-random function initialized by a digital signal (S) representing the supplementary information to be inserted and having means (15) of adding the modulation values (w_k) to the components of said subset.

12. Insertion device according to one of Claims 7 to 11, characterized in that the choosing means (13) for choosing a subset of components cooperate with a generator (16) generating numbers (b_k) according to a pseudo-random function initialized by a digital signal (K) representing a confidential key associated with the supplementary information (S) to be inserted.

13. Insertion device according to one of Claims 7 to 12, characterized in that the means of spectral breakdown (11), extraction (12), choosing (13), modulation (14) and spectral recomposition (15) are incorporated in:

- a microprocessor (10);

- a read-only memory (102) containing a program for inserting a supplementary information item (S); and

- a random access memory (103) containing registers adapted to record variables modified during the running of the program.

14. Method of decoding, in watermarked digital data (I*), a supplementary information item (S), such as a secret watermark, inserted in initial digital data (I) according to the insertion method according to one of Claims 1 to 6, characterized in that it includes the following steps:

- multi-resolution spectral breakdown (E6) of the watermarked digital data (I*) and initial digital data (I);

- extraction (E7) of the components of lowest frequency in the watermarked (I*) and initial digital data (I);

- selection (E8) of the subset of components chosen at the

choosing step (E3) of said method of insertion in the watermarked (I*) and initial digital data (I);

- estimating (E9), by subtraction respectively of the components of said subset of watermarked digital data (I*) from the components of said subset

5 of initial digital data (I), an estimated sequence (W*) of modulation values;

- generation (E10) of a presupposed sequence (W) of modulation values inserted at the modulation step (E4) of said insertion method;

- calculation (E11) of a correlation value between the estimated sequence (W*) and the presupposed sequence (W); and

10 - decision (E12) on the similarity or otherwise of the estimated sequence (W*) and presupposed sequence (W) as a function of said correlation value.

15. Decoding method according to Claim 14, characterized in that, at the spectral breakdown step (E6), the spectral breakdown is effected by a

15 discrete wavelet transformation and, at the extraction step (E7), the components of the approximation sub-band (LL) are chosen.

16. Decoding method according to Claim 14, characterized in that, at the spectral breakdown step (E6), the initial digital data (I) and watermarked digital data (I*) are broken down iteratively into an approximation version

20 corresponding to a low-pass filtering and a sub-sampling of the digital data or of a previous approximation version, and into a detail version corresponding to the subtraction of the approximation version from the digital data or from said previous approximation version, and in that, at the extraction step (E7), the components of the approximation version are chosen.

25 17. Decoding method according to one of Claims 14 to 16, characterized in that, at the generation step (E10), the presupposed sequence (W) of modulation values is generated by a pseudo-random function initialized by a digital signal (S) representing the supplementary information to be decoded.

30 A 18. Decoding method according to one of Claims 14 to 17, characterized in that, at the selection step (E8), the subset of components is chosen according to a pseudo-random function initialized by a digital signal (K)

representing a confidential key associated with the supplementary information (S) to be decoded.

19. Device for decoding, in watermarked digital data (I*), a supplementary information item (S), such as a secret watermark, inserted in initial digital data (I) according to the insertion method according to ~~one of~~ claim 1

~~Claims 1 to 6~~, characterized in that it has:

- means (61) of multi-resolution spectral breakdown of the watermarked digital data (I*) and initial digital data (I);

- means (62) of extraction of the components of lowest frequency in the watermarked (I*) and initial digital data (I);

- means (63) of selection of the subset of components chosen at the choosing step (E3) of said method of insertion in the watermarked (I*) and initial digital data (I);

- means (64) of estimating, by subtraction respectively of the components of said subset of watermarked digital data (I*) from the components of said subset of initial digital data (I), an estimated sequence (W*) of modulation values;

- means (65) of generating a presupposed sequence (W) of modulation values inserted at the modulation step (E4) of said insertion method;

- means (67) of calculating a correlation value between the estimated sequence (W*) and the presupposed sequence (W); and

- means (68) of deciding on the similarity or otherwise of the estimated sequence (W*) and of the presupposed sequence (W) as a function of said correlation value.

20. Decoding device according to Claim 19, characterized in that the spectral breakdown means (61) are adapted to perform a discrete wavelet transformation, the extraction means (62) being adapted to choose the components of the approximation sub-band (LL).

21. Decoding device according to Claim 19, characterized in that the spectral breakdown means (61) are adapted to break down the initial digital data (I) and watermarked digital data (I*) iteratively into an approximation version corresponding to a low-pass filtering and a sub-sampling of the digital

data or of a previous approximation version, and into a detail version corresponding to a subtraction of the approximation version from the digital data or from the said previous approximation version, the extraction means (62) being adapted to choose the components of the approximation version.

5   22. Decoding device according to one of Claims 19 to 21, characterized in that the means (65) of generating the presupposed sequence (W) of modulation values cooperate with a generator (66) generating modulation values generated by a pseudo-random function initialized by a digital signal (S) representing supplementary information to be decoded.

10   23. Decoding device according to one of Claims 19 to 22, characterized in that the selection means (63) cooperate with a generator (66) generating numbers (b_k) in accordance with a pseudo-random function initialized by a digital signal (K) representing a confidential key associated with the supplementary information (S) to be decoded.

15   24. Decoding device according to one of Claims 19 to 23, characterized in that the means of spectral breakdown (61), extraction (62), selection (63), estimation (64), generation (65), calculation (67) and decision (68) are incorporated in:

- a microprocessor (10);

20   - a read-only memory (102) containing a program for decoding a supplementary information item (S); and

- a random access memory (103) containing registers adapted to record variables modified during the running of the program.

25   25. Digital signal processing apparatus, characterized in that it has an insertion device according to one of Claims 7 to 13.

26. Digital signal processing apparatus, characterized in that it has a decoding device according to one of Claims 19 to 24.

27. Digital photographic apparatus, characterized in that it has an insertion device according to one of Claims 7 to 13.

30   28. Digital photographic apparatus, characterized in that it has a decoding device according to one of Claims 19 to 24.

29. Digital camera, characterized in that it has an insertion device

according to one of Claims 7 to 13.

30. Digital camera, characterized in that it has a decoding device according to one of Claims 19 to 24.

31. Database management system, characterized in that it has an insertion device according to one of Claims 7 to 13.

32. Database management system, characterized in that it has a decoding device according to one of Claims 19 to 24.

33. Computer, characterized in that it has an insertion device according to one of Claims 7 to 13.

10

34. Computer, characterized in that it has a decoding device according to one of Claims 19 to 24.

35. Scanner, characterized in that it has an insertion device according to one of Claims 7 to 13.

36. Scanner, characterized in that it has a decoding device 15 according to one of Claims 19 to 24.

37. Medical imaging apparatus, and notably an X-ray radiography apparatus, characterized in that it has an insertion device according to one of Claims 7 to 13.

38. Medical imaging apparatus, and notably an X-ray radiography 20 apparatus, characterized in that it has a decoding device according to one of Claims 19 to 24.

39. Method of inserting a supplementary information item (S), such as a secret watermark, in digital data (I), characterized in that it includes the following steps:

25

- multi-resolution spectral breakdown (E101) of the digital data (I);

- extraction (E102) of the components of a frequency sub-band (LL);

- spectral transformation (E103) of the components of said frequency sub-band (LL);

30

- choice (E104) of a subset of coefficients (X_k) of said spectral transformation;

- modulation (E105) of the coefficients (X_k) of said subset in order

to insert the supplementary information (S);

- reverse spectral transformation (E106) of the coefficients including the subset of modulated coefficients (X'_k); and

- reverse multi-resolution spectral recomposition (E107) of the watermarked digital data (I').

40. Insertion method according to Claim 39, characterized in that, during the extraction step (E102), the components of the sub-band with the lowest frequency (LL) are chosen.

41. Insertion method according to one of Claims 39 or 40, characterized in that, at the spectral breakdown step (E101), the spectral breakdown is effected by a discrete wavelet transformation, and, at the extraction step (E102), the components of the approximation sub-band (LL) are chosen.

42. Insertion method according to Claim 41, characterized in that the level of breakdown by the wavelet transformation is predetermined so that the member (n) of components of the approximation sub-band (LL) is between 8x8 and 32x32.

43. Insertion method according to one of Claims 39 to 42, characterized in that the spectral transformation is a discrete cosine transformation.

44. Insertion method according to one of Claims 39 to 43, characterized in that, at the modulation step (E105), the coefficients (X_k) of said subset are modulated by adding a modulation value (w_k) generated by a pseudo-random function initialized by a digital signal (S) representing the supplementary information to be inserted.

45. Insertion method according to one of Claims 39 to 44, characterized in that, at the choosing step (E104), the subset of coefficients (X_k) is chosen according to a pseudo-random function initialized by a digital signal (K) representing a confidential key associated with the supplementary information (S) to be inserted.

46. Device for inserting a supplementary information item (S), such as a secret watermark, in digital data (I), characterized in that it has:

- means (31) for the multi-resolution spectral breakdown of the digital data (I);

- extraction means (32) adapted to extract components of a frequency sub-band (LL);

5   - means (33) for the spectral transformation of the components of said frequency sub-band (LL);

- choosing means (34) for choosing a subset of coefficients (X_k) of said spectral transformation;

- means (35) of modulating the coefficients (X_k) of said subset in

10   order to insert the supplementary information (S);

- means (36) for the reverse spectral transformation of the coefficients including the subset of modulated coefficients (X'_k) ; and

- means (37) for the reverse multi-resolution spectral recomposition of the watermarked digital data (I').

15   47. Insertion device according to Claim 46, characterized in that the extraction means (32) for extracting a frequency sub-band are adapted to choose the components of the sub-band with the lowest frequency (LL).

48. Insertion device according to one of Claims 46 or 47, characterized in that the multi-resolution spectral breakdown means (31) are

20   adapted to perform a discrete wavelet transformation, the extraction means (32) being adapted to choose the components of the approximation sub-band (LL).

49. Insertion device according to Claim 48, characterized in that the breakdown number (d) for the wavelet transformation is predetermined so that the number (n) of components of the approximation sub-band (LL) is

25   between 8 x 8 and 32 x 32.

50. Insertion device according to one of Claims 46 to 49, characterized in that the spectral transformation means (33) are adapted to effect a discrete cosine transform.

51. Insertion device according to one of Claims 46 to 50,

30   characterized in that the modulation means (35) cooperate with a generator (38) of modulation values (w_k) generated by a pseudo-random function initialized by a digital signal (S) representing the supplementary information to be inserted

and having means (35) of adding the modulation values (w_k) to the coefficients (X_k) of said subset.

52. Insertion device according to one of Claims 46 to 51, characterized in that the choosing means (34) for choosing a subset of coefficients (X_k) cooperate with a generator (38) of numbers (b_k) according to a pseudo-random function initialized by a digital signal (K) representing a confidential key associated with the supplementary information (S) to be inserted.

53. Insertion device according to one of Claims 46 to 52, characterized in that the means of spectral breakdown (31), extraction (32), spectral transformation (33) choosing (34), modulation (35), reverse spectral transformation (36) and spectral recomposition (37) are incorporated in:

- a microprocessor (10),

- a read-only memory (102) containing a program for inserting a supplementary information item (S), and

- a random access memory (103) containing registers adapted to record variables modified during the running of the program.

54. Method of decoding, in watermarked digital data (I*), a supplementary information item (S), such as a secret watermark, inserted in initial digital data (I) according to an insertion method according to one of Claims 39 to 45, characterized in that it includes the following steps:

- multi-resolution spectral breakdown (E110) of the watermarked digital data (I*) and initial digital data (I);

- extraction (E111) of the components of a sub-band of frequencies (LL) respectively in the watermarked (I*) and initial (I) digital data;

- spectral transformation (E112) of the components of the frequency sub-band (LL) of the watermarked digital data (I*) and initial digital data (I).

- selection (E113) of the subset of coefficients chosen at the choosing step (E104) of said method of insertion in the watermarked digital data (I*) and initial digital data (I);

- estimating (E114), by subtraction respectively of the coefficients

of said subset of watermarked digital data (I*) from the coefficients of said subset of initial digital data (I), an estimated sequence (W*) of modulation values;

    - generation (E115) of a presupposed sequence (W) of modulation values inserted at the modulation step (E105) of said insertion method;

    - calculation (E116) of a value of correlation between the estimated sequence (W*) and the presupposed sequence (W); and

    - deciding (E117) on the similarity or otherwise of the estimated sequence (W*) and presupposed sequence (W) as a function of said correlation value.

    55. Decoding method according to Claim 54, characterized in that, during the extraction step (E111), the components of the sub-band with the lowest frequency (LL) are chosen.

    56. Decoding method according to one of Claims 54 or 55, characterized in that, at the spectral breakdown step (E110), the spectral breakdown is effected by means of a discrete wavelet transformation and, at the extraction step (E111), the components of the approximation sub-band (LL) are chosen.

    57. Decoding method according to one of Claims ~~54 to 56~~ 54 or 55, characterized in that the spectral transformation is a discrete cosine transform.

    58. Decoding method according to one of Claims ~~54 to 57~~ 54 or 55, characterized in that, at the generation step (E115), the presupposed sequence (W) of modulation values is generated by means of a pseudo-random function initialized by a digital signal (S) representing the supplementary information to be decoded.

    59. Decoding method according to one of Claims ~~54 to 58~~ 54 or 55, characterized in that, at the selection step (E113), the subset of coefficients is chosen according to a pseudo-random function initialized by a digital signal (K) representing a confidential key associated with the supplementary information (S) to be decoded.

    60. Device for decoding, in watermarked digital data (I*), a supplementary information item (S), such as a secret watermark, inserted in

A initial digital data (I) according to an insertion method in accordance with ~~one of~~
Claim 39
A ~~Claims 39 to 45,~~ characterized in that it has:

- means (21) of multi-resolution spectral breakdown of the watermarked digital data (I*) and initial digital data (I);

5   - means (22) of extraction of the components of a sub-band of frequencies (LL) respectively in the watermarked (I*) and initial (I) digital data;

- means (23) for the spectral transformation of the components of the frequency sub-band (LL) of the watermarked digital data (I*) and initial digital data (I);

10   - means (24) of selection of the subset of coefficients chosen at the choosing step (E104) of said method of insertion in the watermarked (I*) and initial (I) digital data;

- means (25) of estimating, by subtraction respectively of the coefficients of said subset of watermarked digital data (I*) from the coefficients of said subset of initial digital data (I), an estimated sequence (W*) of
15   modulation values;

- means (26) of generating a presupposed sequence (W) of modulation values inserted at the modulation step (E105) of said insertion method;

20   - means (28) of calculating a value of correlation between the estimated sequence (W*) and the presupposed sequence (W); and

- means of deciding (29) on the similarity or otherwise of the estimated sequence (W*) and of the presupposed sequence (W) as a function of said correlation value.

25   61. Decoding device according to Claim 60, characterized in that the extraction means (22) are adapted to choose the components of the sub-band with the lowest frequency (LL).

62. Decoding device according to one of Claims 60 or 61, characterized in that the multi-resolution spectral breakdown means (21) are
30   adapted to effect a discrete wavelet transformation, the extraction means (22) being adapted to choose the components of the approximation sub-band (LL).
60 or 61
A   63. Decoding device according to one of Claims ~~60 to 62,~~

characterized in that the spectral transformation means (23) are adapted to effect a discrete cosine transform.

64. Decoding device according to one of Claims 60 to 63, characterized in that the generation means (26) cooperate with a generator (27) of modulation values generated by means of a pseudo-random function initialized by a digital signal (S) representing the supplementary information to be decoded.

65. Decoding device according to one of Claims 60 to 64, characterized in that the selection means (24) cooperate with a generator (27) of numbers (b_k) in accordance with a pseudo-random function initialized by a digital signal (K) representing a confidential key associated with the supplementary information (S) to be decoded.

66. Decoding device according to one of Claims 60 to 65, characterized in that the means of spectral breakdown (21), extraction (22), spectral breakdown (23), selection (24), estimation (25), generation (26), calculation (28) and decision (29) are incorporated in:

- a microprocessor (10),

- a read-only memory (102) containing a program for decoding a supplementary information item (S), and

- a random access memory (103) containing registers adapted to record variables modified during the running of the program.

67. Digital signal processing apparatus, characterized in that it has an insertion device according to one of Claims 46 to 53.

68. Digital signal processing apparatus, characterized in that it has a decoding device according to one of Claims 60 to 66.

69. Digital photographic apparatus, characterized in that it has an insertion device according to one of Claims 46 to 53.

70. Digital photographic apparatus, characterized in that it has a decoding device according to one of Claims 60 to 66.

71. Digital camera, characterized in that it has an insertion device according to one of Claims 46 to 53.

72. Digital camera, characterized in that it has a decoding device

A according to one of Claims 60 to 66. *(handwritten: 60 or 61)*

73. Database management system, characterized in that it has an
A insertion device according to one of Claims 46 to 53. *(handwritten: 46 or 47)*

74. Database management system, characterized in that it has a
A 5 decoding device according to one of Claims 60 to 66. *(handwritten: 60 or 61)*

75. Computer, characterized in that it has an insertion device
A according to one of Claims 46 to 53. *(handwritten: 46 or 47)*

76. Computer, characterized in that it has a decoding device
A according to one of Claims 60 to 66. *(handwritten: 60 or 61)*

10

77. Scanner, characterized in that it has an insertion device
according to one of Claims 46 to 53. *(handwritten: 46 or 47)*

78. Scanner, characterized in that it has a decoding device
A according to one of Claims 60 to 66. *(handwritten: 60 or 61)*

79. Medical imaging apparatus, and notably an X-ray radiography
15 apparatus, characterized in that it has an insertion device according to one of
A Claims 46 to 53. *(handwritten: 46 or 47)*

80. Medical imaging apparatus, and notably an X-ray radiography
apparatus, characterized in that it has a decoding device according to one of
A Claims 60 to 66. *(handwritten: 60 or 61)*

20